

## Mapping of COSO, CobiT 4.1 & ISO 27002:2005

COSO	CobiT 4.1	ISO 27002:2005
1. CONTROL ENVIRONMENT (1.1) RISK-APPROACH (1.2) CONTROL ACTIVITIES (1.3) MONITORING	101 Strategic risk and control 102 Identification of all control responsibilities 103 Support leadership management	5.1.1 Identification of risks subject to control process 5.1.2 Addressing security in third-party agreements 5.1.3 Managing changes in third-party services 5.1.4 Data protection and privacy of personal information
	104 Support performance monitoring	5.1.5 Addressing security in third-party agreements 5.1.6 Service delivery 5.1.7 Monitoring and review of third-party services 5.1.8 Protection of operational data 5.1.9 Information security assessment
	105	
	106	
2. CONTROL ACTIVITIES (2.1) IDENTIFY (2.2) DESIGN (2.3) IMPLEMENT (2.4) MONITOR (2.5) EVALUATE (2.6) IMPROVE	201 Strategic and business continuity 202 Information security planning 203 Asset protection and control 204 Access protection and security 205 Business continuity security 206 IT security framework 207 IT security plans 208 Global IT resources 209 Maintenance of the IT security plan 210 Testing, training, and measuring business continuity plans 211 IT security plan testing 212 Maintenance of the IT security plan 213 IT services recovery/backup 214 Data backup storage 215 Data recovery review	5.2.1 Capacity management 5.2.2 Capacity management 5.2.3 Capacity management 5.2.4 Capacity management 5.2.5 Capacity management 5.2.6 Capacity management 5.2.7 Capacity management 5.2.8 Capacity management 5.2.9 Capacity management 5.2.10 Capacity management 5.2.11 Capacity management 5.2.12 Capacity management 5.2.13 Capacity management 5.2.14 Capacity management 5.2.15 Capacity management 5.2.16 Capacity management 5.2.17 Capacity management 5.2.18 Capacity management 5.2.19 Capacity management 5.2.20 Capacity management 5.2.21 Capacity management 5.2.22 Capacity management 5.2.23 Capacity management 5.2.24 Capacity management 5.2.25 Capacity management 5.2.26 Capacity management 5.2.27 Capacity management 5.2.28 Capacity management 5.2.29 Capacity management 5.2.30 Capacity management 5.2.31 Capacity management 5.2.32 Capacity management 5.2.33 Capacity management 5.2.34 Capacity management 5.2.35 Capacity management 5.2.36 Capacity management 5.2.37 Capacity management 5.2.38 Capacity management 5.2.39 Capacity management 5.2.40 Capacity management 5.2.41 Capacity management 5.2.42 Capacity management 5.2.43 Capacity management 5.2.44 Capacity management 5.2.45 Capacity management 5.2.46 Capacity management 5.2.47 Capacity management 5.2.48 Capacity management 5.2.49 Capacity management 5.2.50 Capacity management 5.2.51 Capacity management 5.2.52 Capacity management 5.2.53 Capacity management 5.2.54 Capacity management 5.2.55 Capacity management 5.2.56 Capacity management 5.2.57 Capacity management 5.2.58 Capacity management 5.2.59 Capacity management 5.2.60 Capacity management 5.2.61 Capacity management 5.2.62 Capacity management 5.2.63 Capacity management 5.2.64 Capacity management 5.2.65 Capacity management 5.2.66 Capacity management 5.2.67 Capacity management 5.2.68 Capacity management 5.2.69 Capacity management 5.2.70 Capacity management 5.2.71 Capacity management 5.2.72 Capacity management 5.2.73 Capacity management 5.2.74 Capacity management 5.2.75 Capacity management 5.2.76 Capacity management 5.2.77 Capacity management 5.2.78 Capacity management 5.2.79 Capacity management 5.2.80 Capacity management 5.2.81 Capacity management 5.2.82 Capacity management 5.2.83 Capacity management 5.2.84 Capacity management 5.2.85 Capacity management 5.2.86 Capacity management 5.2.87 Capacity management 5.2.88 Capacity management 5.2.89 Capacity management 5.2.90 Capacity management 5.2.91 Capacity management 5.2.92 Capacity management 5.2.93 Capacity management 5.2.94 Capacity management 5.2.95 Capacity management 5.2.96 Capacity management 5.2.97 Capacity management 5.2.98 Capacity management 5.2.99 Capacity management 5.3.00 Capacity management



## Recommendations

- An IT framework and governance should be planned for the life cycle of the organization, enhance the system of internal control to conform to SOX, and result in more accurate, reliable, and timely financial reporting

- A strong IT internal control program can assist organizations in gaining a competitive edge through efficiency and effectiveness of operations, improve management competencies, prioritize organizational goals, prevent loss of information assets, and increase public trust in financial statement reporting and protection of assets

- Relying solely on COSO may result in organizations failing to consider risks that exist within a system... CobiT 4.1 provides a more detailed explanation of SOX requirements but provides no specific guidelines for implementation

ISO 27000 provides specific, comprehensive objectives that can be accomplished within an organization to ensure SOX compliance

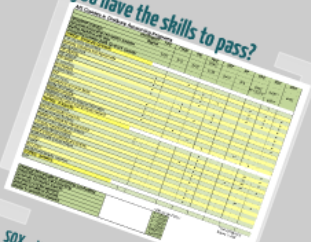
## CPA Exam IT Competencies

- SOX requirements
- COSO framework
- Procedures to assess the control environment
- Entity-level controls & their ability to mitigate risks
- Business processes, documentation & information flows
- Effect of IT on the effectiveness of internal controls
- Design & implementation of internal controls
- Change management, backup, recovery & network access
- Application functionality, application access control, controls over interfaces, integrations & eCommerce
- Significant algorithms, reports, validation, edit checks & error handling



# SOX Deficiency in IT controls & security

Do you have the skills to pass?



Control	Frequency	Responsible Party	Status
1. Financial reporting process	Quarterly	Finance Dept	Compliant
2. Internal control over financial reporting	Quarterly	Finance Dept	Compliant
3. Information security	Quarterly	IT Dept	Compliant
4. Access to financial data	Quarterly	IT Dept	Compliant
5. Backup and recovery	Quarterly	IT Dept	Compliant
6. Disaster recovery	Quarterly	IT Dept	Compliant
7. Business continuity	Quarterly	IT Dept	Compliant
8. Risk management	Quarterly	IT Dept	Compliant
9. Change management	Quarterly	IT Dept	Compliant
10. Incident response	Quarterly	IT Dept	Compliant

## SOX... We all know it

- Not Sarbanes Oxley Act of 2002
- It's a regulation was enacted by the financial standards of the early 2000s
- Legislation that affects public companies and the public accounting firms who audit them

The SOX Top  
<http://www.sec.gov/edgar/disclosure/otherdocs/sox/sox.htm>

## Examples of IT Security Failures

### Citibank

- \$2.7 million in fraudulent losses
- Hackers obtained account information from the website
- Account numbers appeared in web address browser bar

Did Citibank implement sufficient IT Security?

Were they demonstrating compliance with SOX?

All of these firms:

- Had security procedures in place, BUT...Failed to monitor them
- Did not appropriately assess the risks
- Demonstrated a general lack in IT knowledge and/or resources

### Subway

Customer data hacked from POS systems

\$3 million in fraud charges

POS passwords were easily broken

Customer's credit cards should further secure

### TJX, Inc.

Unauthorized intrusion into its networks

Over 100 million accounts accessed over 17

### TJX

Problems?

- Outdated wireless security encryption system
- Failed to install firewalls and encrypt computers
- Did not properly install additional security layer

# SOX... We all know it

- The Sarbanes-Oxley Act of 2002
- It's creation was motivated by the financial scandals of the early 2000's
- Legislation that affects public companies and the public accounting firms who audit them

The SOX rap:

<http://www.dailynugget.com/2004/12/clockin-lots-of-hours-on-section-404/>

# SOX and IT

- Section 404 - Internal control requirements, which include IT controls
- Public companies must implement controls, and together with their auditors, must report on their efficiency and effectiveness on the accuracy of financial reporting
- "This is the most costly aspect of the legislation for companies to implement, as documenting and testing important financial manual and automated controls requires enormous effort." - Wikipedia

# SOX and IT

- Can be vague, as it does not provide a required control framework or IT specific guidance for implementation
- The SEC released their interpretive guidance in 2007
  - Recommends the use of the COSO framework
- The PCAOB approved Auditing Standard No. 5 in 2007 to provide guidance for implementation
  - Supersedes Auditing Standard No. 2 from 2004
  - The COSO report

# Our Goal

- To analyze IT controls and security implementation and its relationship with financial reporting, highlighting the need for better guidance
  - Examples of IT security failures
  - Discussion of control frameworks
  - Our recommendation for better guidance

Keep chuggin' along I've heard all your pains  
I know the days are long and the nights are short  
But it's really sad that people try to extort  
And we couldn't let things keep goin' on  
Cuz there's a lot of companies like Enron  
Yea the list is long but we think it's for the best  
We had to make it safe for everyone to invest  
Yea well my name is Mike last name Oxley  
Some think it's overkill but please don't knock me  
We had to protect investors from fraud  
We wanna minimize the risk for anyone could rob  
I think me and Paul finally got it figured out  
But I'm sure some of you will continue to doubt  
We knew there was something that we had to do  
And now you got the Sarbanes-Oxley Act of 2002

Clockin' lots of hours on section 404, I go to work early and I get home late  
Clockin' lots of hours on section 404, No time to waste, can't miss the due date  
Clockin' lots of hours on section 404, I can pretty much kiss my vacation goodbye  
Clockin' lots of hours on section 404, I wish my fiscal year ended in July

I'm the SEC so don't mess with me  
I'm gonna tell you 'bout the PCAOB  
They're gonna show up at your front door,  
Checkin' out your section 404

So you gotta make sure that you get done  
And I know for sure it's not gonna be fun  
You need to buckle down, you need to get your mind straight  
Cuz this is something that really just can't wait

Yea we're the SEC and we're not

# Examples of IT Security Failures

## Citibank

- **\$2.7 million in fraudulent losses**
- **Hackers obtained account information from the website**
- **Account numbers appeared in web address browser bar**



Did Citibank implement sufficient IT Security?

Were they demonstrating compliance with SOX?

# TJX, Inc.

Unauthorized intrusion into its networks

Over 100 million accounts accessed over 17 months

Had to pay nearly \$500 million in lawsuits and settlements

# TJX

## Problems?

- Outdated wireless security encryption system
- Failed to install firewalls and encrypt computers
- Did not properly install additional security layer

# Subway

Customer data hacked from POS systems

\$3 million in fraud charges

POS passwords were easily broken

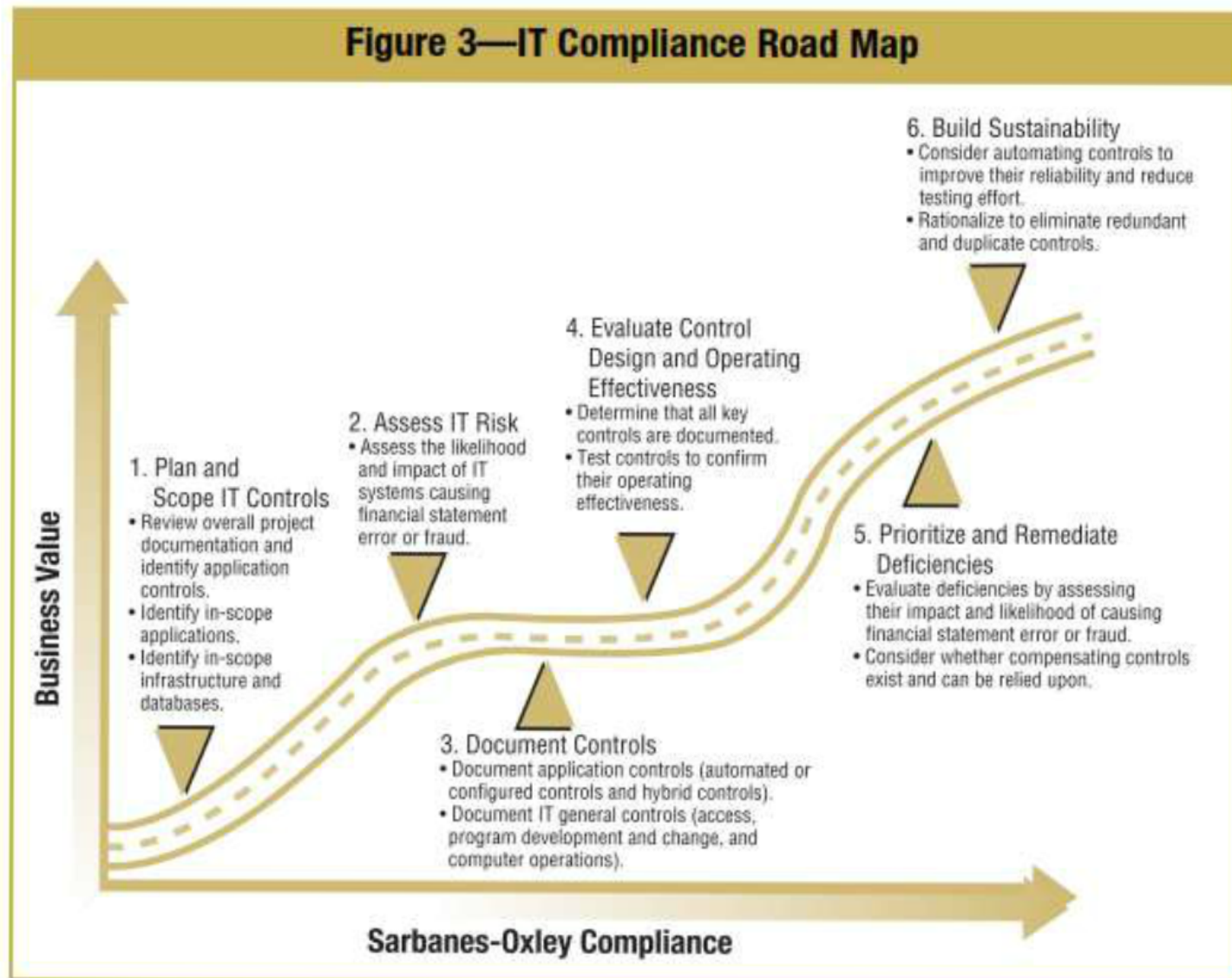
Keyloggers & backdoors allowed further access

All of these firms:

- Had security procedures in place, BUT...Failed to monitor them
- Did not appropriately assess the risks
- Demonstrated a general lack in IT Security knowledge (e.g. secure passwords, firewalls)

# COSO, CobiT, and ISO 27000

**Figure 3—IT Compliance Road Map**



# COSO

- Internal Control-Integrate Framework Report from the Committee Of Sponsoring Organizations of the Treadway Committee
- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring

## Recommended by the SEC for SOX compliance BUT...

- Focuses BROADLY on internal controls
- Target audience is management
- Can result in materially wrong conclusions
- Obsolete
- Does not address commitment goals, defining & communicating objectives, measurement, continuity of business, management's role in overseeing effectiveness of IT risk management and control
- Focuses only on the entity level



# CobiT

- Control **OB**jectives for **I**nformation and related **T**echnology
- Plan & Organize
- Acquire & Implement
- Deliver & Support
- Monitor & Evaluate
- 34 High Level Control Objectives
- 215 Control Processes

## ISO 27001

- "plan-do-check-act" cycle
- establish, implement, maintain, & review, improve the ISMS
- Targets e

**Figure 9—Cross-reference of COSO and COBIT Control Components**



# Can be used with COSO but...

- Focus on IT function in terms of quality and security requirements
- Target audience is management, auditors, financial statement users
- Does not include specific implementation guidance



# ISO 27000

- "plan-do-check-act" cycle... PDCA
- establish, implement & operate, monitor & review, maintain & improve the ISMS
- Targets everyone involved with an organization
- Specific, comprehensive objectives that can be accomplished to ensure SOX compliance

# Mapping of COSO, CobiT 4.1 & ISO 27002:2005

COSO	CobiT 4.1	ISO/IEC 27002:2005
1. CONTROL ENVIRONMENT	DS2 <i>Manage third party services</i>	
2. RISK ASSESSMENT	DS2.1 Identification of all supplier relationships	6.2.1 Identification of risks related to external parties
3. CONTROL ACTIVITIES	DS2.2 Supplier relationship management	6.2.3 Addressing security in third party agreements 10.2.3 Managing changes to third party services 15.1.4 Data protection and privacy of personal information
5. MONITORING	DS2.4 Supplier performance monitoring	6.2.3 Addressing security in third party agreements 10.2.1 Service delivery 10.2.2 Monitoring and review of third party services 12.4.2 Protection of system test data 12.5.5 Outsourced software development
3. CONTROL ACTIVITIES	DS3 <i>Manage performance/capacity</i>	
5. MONITORING	DS3.1 Performance/capacity planning	10.3.1 Capacity management
	DS3.2 Current performance/capacity	10.3.1 Capacity management
	DS3.3 Future performance/capacity	10.3.1 Capacity management
	DS4 <i>Ensure continuous security</i>	
	DS4.1 IT continuity framework	6.1.6 Contact with authorities 6.1.7 Contact with special interest groups 14.1.1 continuity management risk assessment 14.1.2 Business continuity and risk assessment 14.1.4 Business continuity planning framework
	DS4.2 IT continuity plans	6.1.6 Contact with authorities 6.1.7 Contact with special interest groups 14.1.3 Developing and implementing continuity plans including information security
	DS4.3 Critical IT resources	14.1.1 Including information security in the business continuity management risk assessment 14.1.2 Business continuity and risk assessment
	DS4.4 Maintenance of the IT continuity plan	14.1.5 Testing, maintaining, and reassessing business continuity plans
	DS4.5 Testing the IT continuity plan	14.1.5 Testing, maintaining, and reassessing business continuity plans
	DS4.6 IT continuity plan training	14.1.5 Testing, maintaining, and reassessing business continuity plans
	DS4.7 Distribution of the IT continuity plan	14.1.5 Testing, maintaining, and reassessing business continuity plans
	DS4.8 IT services recovery/resumption	14.1.1 Including information security in the business continuity management risk assessment 14.1.3 Maintain or restore operations and ensure availability of information
	DS4.9 Offsite backup storage	10.5.1 Information backup
	DS4.10 Post resumption review	14.1.5 Testing, maintaining, and reassessing business continuity plans

# CPA Exam IT Competencies

- SOX requirements
- COSO framework
- Procedures to assess the control environment
- Entity-level controls & their ability to mitigate risks
- Business processes, documentation & information flows
- Effect of IT on the effectiveness of internal controls
- Design & implementation of internal controls
- Change management, backup, recovery & network access
- Application functionality, application access control, controls over interfaces, integrations & eCommerce
- Significant algorithms, reports, validation, edit checks & error handling

# Do you have the skills to pass?

## AIS Courses in Graduate Accounting Programs

UNIVERSITY Degree	FAU	FGCU	FIU	FSU Macc*	UCF	UF	UNF	USF	UWF
<b>REQUIRED COURSE:</b>									
<b>Advanced Accounting Information Systems</b>	6475	N/A	6437	5138	6415	N/A	6405	6476**	6405
<b>Making Decisions with Data</b>							ECO5415^		
<b>Accounting Systems Audit, Control &amp; Security</b>								6457^	
<b>TOPICS: Broad AIS Concepts</b>									
The role of the accountant								•	
Business processes and requirements			•						
AIS development	•			•			•	•	•
AIS planning	•			•	•		•	•	•
AIS analysis	•			•			•	•	•
AIS design	•			•			•	•	•
IT resources	•		•		•				•
IT processes			•		•				•
IT governance			•		•				•
ERP	•			•					•
eCommerce	•								•
Advanced eCommerce topics	•								
eData interchange	•								
Database concepts	•		•						
Statistical methods for financial information				•			•^		
Contemporary and emerging issues research					•			•	
<b>TOPICS: IT Security</b>									
Virtual Environment					•				•
Information systems security	•				•			•^	•
Advanced security topics	•				•			•^	•
Statistical methods for internal control				•	•			•^	
Internal control design and analysis					•		•	•^	•
Computer fraud and abuse					•				
Fraud and internal controls					•				
Ethical choices in planning and controls					•				
Audit concepts and techniques								•^	•
COSO					•				
CoBIT					•				
ISO 27001					•				
Incident and disaster response					•				
<b>TOPICS: Software</b>									
SAP	•								

\*AIS concentration

\*\*Contemporary  
Issues in AIS

Emerging Technologies in Accounting and Auditing

ACG5458

Enterprise Systems and Accounting

ACG5505

Corporate Information Security

ACG5525



# Recommendations

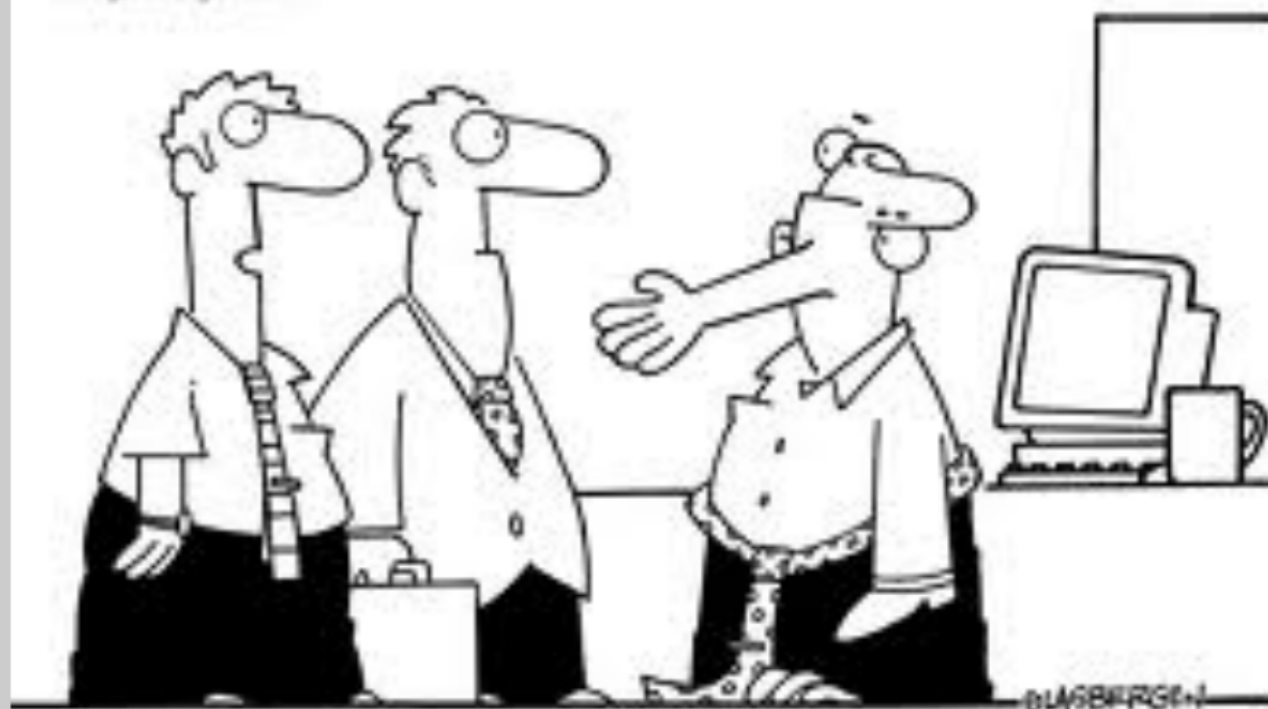
- An IT framework and governance should be planned for the life cycle of the organization, enhance the system of internal control to conform to SOX, and result in more accurate, reliable, and timely financial reporting
- A strong IT internal control program can assist organizations in gaining a competitive edge through efficiency and effectiveness of operations, improve management competencies, prioritize organizational goals, prevent loss of information assets, and increase public trust in financial statement reporting and protection of assets
  - Relying solely on COSO may result in organizations failing to consider risks that exist within a system... CobiT 4.1 provides a more detailed explanation of SOX requirements but provides no specific guidelines for implementation



ISO 27000 provides specific,  
comprehensive objectives that can be  
accomplished within an organization  
to ensure SOX compliance



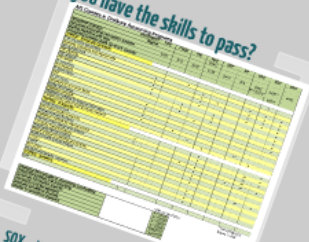
Copyright 2002 by Randy Glasbergen.  
www.glasbergen.com



"That's our CIO. He's encrypted for security purposes."

# SOX Deficiency in IT controls & security

Do you have the skills to pass?



Control	Frequency	Responsible	Reviewed	Compliant
1. All financial data is properly recorded and maintained.	Quarterly	John Doe	12/15/2003	Yes
2. All financial data is properly reviewed and approved.	Quarterly	Jane Smith	12/15/2003	Yes
3. All financial data is properly reconciled and balanced.	Quarterly	Bob Johnson	12/15/2003	Yes
4. All financial data is properly audited and verified.	Quarterly	Alice Brown	12/15/2003	Yes
5. All financial data is properly reported and disclosed.	Quarterly	Charlie Davis	12/15/2003	Yes

## SOX... We all know it

- Not Sarbanes-Oxley Act of 2002
- It's a regulation was enacted by the financial scandals of the early 2000s
- Legislation that affects public companies and the public accounting firms who audit them

The SOX Top  
<http://www.dhs.gov/sox-top>  
SEC

## Examples of IT Security Failures

### Citibank

- \$2.7 million in fraudulent losses
- Hackers obtained account information from the website
- Account numbers appeared in web address browser bar

Did Citibank implement sufficient IT Security?

Were they demonstrating compliance with SOX?

All of these firms:

- Had security procedures in place, BUT...Failed to monitor them
- Did not appropriately assess the risks
- Demonstrated a general lack in IT knowledge and/or resources

### Subway

Customer data hacked from POS systems

\$3 million in fraud charges

POS passwords were easily broken

Customer's credit cards should further secure

### TJX, Inc.

Unauthorized intrusion into its networks

Over 100 million accounts accessed over 17

### TJX

Problems?

- Outdated wireless security encryption system
- Failed to install firewalls and encrypt computers
- Did not properly install additional security layer